27 April 1982

MEMORANDUM FOR: [redacted] 25X1
Chief, Office of Security, Policy & Plans, P&M

SUBJECT: National Security Study Directive 2/82

1. Attached for your information are an "Outline for National Security Study Directive 2/82 Study" and "Definitions for Terms of Reference and Outline for NSSD 2/82 Study".

2. Additional information on NSSD 2/82 will be forwarded to you in the future. Any questions regarding the Study may be addressed to [redacted] on 25X1
extension [redacted] 25X1

[redacted] 25X1

Attachments:
As Stated

OS REGISTRY
0s2 1123

OS REGISTRY
FILE

Next 1 Page(s) In Document Denied

Approved For Release 2008/07/23 : CIA-RDP86B01123R000100070012-0

UNCLASSIFIED

Attachment A

DEFINITIONS FOR TERMS OF REFERENCE AND OUTLINE FOR NSSD 2/82 STUDY

Threat or Intelligence Threat: The combination of capability and intent on the part of a foreign country to engage in an intelligence activity inimical to the United States.

Multidisciplinary Threat: The aggregate, irrespective of collection method or technique, of all the intelligence threats posed by a given country or country group.

Vulnerability: The potential for information to be acquired through intelligence activity. Vulnerability is independent of the threat, i.e., a vulnerability may exist even though no capability or intent exists to exploit it.

Security: Establishment and maintenance of protective measures which are intended to ensure a state of inviolability from hostile acts or influences. Security requirements typically establish a required level of protection based on vulnerability rather than threat.

Communications Security: The application of security to deny unauthorized persons information which might be derived from telecommunications or to ensure the authenticity of telecommunications.

Personnel Security: The application of security to assure that persons granted access to information are loyal and trustworthy.

Physical Security: The use of guards, barriers, containers, alarms and other physical means to protect material, facilities or documents from damage, theft or unauthorized access.

Document Security: The protection of documents through the use of classification designators and their associated access controls.

Computer Security (also Automatic Data Processing Security): The protection of computers and data processing equipment and the information they contain through a combination of physical, personnel and communications security, as well as hardware, software and management controls.

Operations Security: The protection of an operation, project or program from hostile intelligence activities. Operations security establishes protective requirements based upon a comparison of vulnerabilities and the multidisciplinary threat. Operations security differs from other security programs in that it focuses on the threat.

UNCLASSIFIED

Counterintelligence: "...information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs." (E.O. 12333) Counterintelligence differs from security in that it is normally directed against a specific known or postulated threat.

Intelligence Countermeasures: The aggregate of all measures taken to provide protection from the intelligence activities, irrespective of method or technique, of foreign countries. Intelligence countermeasures include counterintelligence, operations security, and security. (Also called multidisciplinary counterintelligence).

Active Measures: A Soviet term for activities beyond traditional diplomacy which are used to achieve Soviet foreign policy objectives. Active measures are most frequently carried out by the intelligence services and are intended to influence the policies of foreign governments, disrupt relations between other nations, undermine confidence in foreign leaders and institutions or discredit opponents.